HP Universal CMDB 9.10 Configuration Manager

Windows オペレーティング・システム向け

デプロイメント・ガイド

ドキュメント・リリース日 : 2010 年 11 月
ソフトウェア・リリース日 : 2010 年 11 月

ご注意

保証

HP の製品，またはサービスの保証は，当該製品，およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載で追加保証を意図するものは一切ありません。ここに含まれる技術的，編集上の誤り，または欠如について，HP はいかなる責任も負いません。

ここに記載する情報は，予告なしに変更されることがあります。

権利の制限

機密性のあるコンピュータ・ソフトウェアです。これらを所有，使用，または複製するには，HP からの有効な使用許諾が必要です。商用コンピュータ・ソフトウェア，コンピュータ・ソフトウェアに関する文書類，および商用アイテムの技術データは，FAR 12.211 および 12.212 の規定に従い，ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

ドキュメントの更新情報

このガイドの表紙には，次の識別情報が記載されています。

- ドキュメント・リリース日は，ドキュメントが更新されるたびに変更されます。
- ソフトウェア・リリース日は，このバージョンのソフトウェアのリリース期日を表します。

最新の更新のチェック，またはご使用のドキュメントが最新版かどうかのご確認には，次のサイトをご利用ください。

http://support.openview.hp.com/selfsolve/manuals

このサイトを利用するには，HP Passport への登録とサインインが必要です。HP Passport ID の取得登録は，次の Web サイトから行なうことができます。

http://h20229.www2.hp.com/passport-registration.html（英語サイト）

または，HP Passport のログイン・ページの［**New users - please register**］リンクをクリックします。

適切な製品サポート・サービスをお申し込みいただいたお客様は，最新版をご入手いただけます。詳細は，HP の営業担当にお問い合わせください。

サポート

HP ソフトウェア・サポート Web サイトを参照してください。

http://support.openview.hp.com

HP ソフトウェアが提供する製品，サービス，サポートに関する詳細情報をご覧いただけます。

HP ソフトウェア・サポート・オンラインでは，セルフソルブ機能を提供しています。お客様の業務の管理に必要な対話型の技術支援ツールに素早く効率的にアクセスいただけます。HP ソフトウェア・サポート Web サイトのサポート範囲は次のとおりです。

- 関心のある技術情報の検索
- サポート・ケースとエンハンスメント要求の登録とトラッキング
- ソフトウェア・パッチのダウンロード
- サポート契約の管理
- HP サポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェア・カスタマとの意見交換
- ソフトウェア・トレーニングの検索と登録

一部を除き，サポートのご利用には，HP Passport ユーザとしてご登録の上，ログインしていただく必要があります。また，多くのサポートのご利用には，サポート契約が必要です。HP Passport ID を登録するには，次の Web サイトを参照してください。

http://h20229.www2.hp.com/passport-registration.html（英語サイト）

アクセス・レベルの詳細については，次の Web サイトを参照してください。

http://support.openview.hp.com/access_level.jsp

目次

第 1 章

インストールと構成

本章の内容

Configuration Manager概要

HP Universal CMDB Configuration Manager（Configuration Manager とします）は，CMS のデータの分析と管理を実行するツールです。また，各種データ・ソースや幅広い製品およびアプリケーションにも対応できる CMS インフラストラクチャを管理するための環境を実現します。

エンタープライズ・ネットワーク環境に Configuration Manager をデプロイするためには，リソースの計画やシステム・アーキテクチャの設計が必要になります。Configuration Manager をインストールする前に，本項で記載されているシステム要件などの内容をレビューしてください。

Configuration Manager のシステム要件

サーバのシステム要件

次の表は，Configuration Manager サーバのシステム要件を示しています。

CPU	Intel Pentium 4，4 コア以上
メモリ（RAM）	4 GB 以上
プラットフォーム	x64
オペレーティング・システム	次の 64 ビット Windows オペレーティング・システムがサポート対象です。 ➤ Windows 2003 Enterprise SP2 および R2 SP2 ➤ Windows 2008 Enterprise SP2 および R2

データベース	➤ Microsoft SQL Server 2005 SP2 2005 互換モード 80 （すべて Enterprise エディション） ➤ Oracle 11.1.x
HP Universal CMDB	➤ HP Universal CMDB バージョン 9.03 （一般的な CMDB インストール） このバージョンの詳細なシステム要件については，HP Universal CMDB のドキュメントを参照してください。

クライアントの要件

次の表は，クライアントで Configuration Manager を表示するためのシステム要件を示しています。

ブラウザ	➤ Microsoft Internet Explorer 7.0，8.0 ➤ Mozilla Firefox 3.x
Flash Player ブラウザ・プラグイン	Flash Player 9 以降
画面の解像度	➤ 1024x768 以上 ➤ 1280x1024 を推奨
画面の色	16 ビット以上

推奨されるセットアップ・ガイドライン

次の表は, Configuration Manager のセットアップ・オプションのガイドラインを示します。

LDAP	次の LDAP 環境がサポート対象です。 ➤ Active Directory ➤ SunONE 6.x
データベース・スキーマの最小サイズ（推奨値）	2 GB

Configuration Manager の設定の上限値

次の表は，Configuration Manager の設定の上限値を示します。

ビューの最大数（推奨値）	100
ポリシーの最大数（推奨値）	300
ビューあたりの複合 CI の最大数（推奨値）	5000
同時ユーザの最大数（推奨値）	50

データベースまたはユーザ・スキーマの構成

Configuration Manager の操作には，データベース・スキーマが必要です。Configuration Manager では，Microsoft SQL Server と Oracle Database Server がサポートされています。このタスクでは，Configuration Manager のデータベース・スキーマまたはユーザ・スキーマの接続プロパティをインストール・ウィザードを使って設定する方法を説明します。

注：Microsoft SQL Server と Oracle Server でのシステム要件については，8ページ「サーバのシステム要件」を参照してください。

データベースを構成するには，次の手順を実行します。

1 Microsoft SQL Server データベースまたは Oracle Server ユーザ・スキーマのいずれかを割り当てます。

- **Microsoft SQL Server 2005：**スナップショット分離を有効にします。

  データベースの作成後，次のコマンドを 1 回実行します。

  ```
  alter database ＜ ccm データベース名＞ set read_committed_snapshot on
  ```

  SQL Server のスナップショット分離機能の詳細については，http://msdn.microsoft.com/ja-jp/library/tcbchxcb(VS.80).aspx を参照してください。

- **Oracle：**Oracle ユーザに，**Connect** 役割と **Resource** 役割のみを割り当てます（**Select any table** 権限を割り当てると，スキーマのカタログ作成が失敗します）。

2 次の表では，この構成プロセスで必要になる情報を示しています。内容を確認してください。

✔	必要な情報
	DB ホスト名とポート
	DB ユーザ名とパスワード
	MS SQL：データベース名
	Oracle：SID

3 Configuration Manager インストール・ウィザードを実行します。詳細については，12ページ「Configuration Manager のインストール」を参照してください。

Configuration Manager のインストール

このタスクでは，サーバ上に Configuration Manager をインストールする方法と，データベース接続および UCMDB との統合の設定方法を説明します。ウィザードのページで［**ヘルプ**］をクリックすると，インストールに関するヘルプを参照できます。ウィザードのページの詳細な説明については，21 ページ「Configuration Manager Post Installation Configuration ウィザード」を参照してください。

Configuration Manager をインストールするには，次の手順を実行します。

1 Configuration Manager DVD のルート・ディレクトリで **install.bat** ファイルを探します。

2 ファイルをダブルクリックすると，Configuration Manager インストール・ウィザードが実行されます。

3 ［**Next**］をクリックすると［License Agreement］ページが開きます。

4 License Agreement の条件に同意し，［**Next**］をクリックすると，製品のインストール・ページが開きます。

5 インストールする製品（UCMDB と Configuration Manager）を選択し，インストール先を指定します。UCMDB ライセンスをカスタマイズする場合は，該当するチェック・ボックスを選択します。［**Next**］をクリックすると，UCMDB のインストールが始まります。UCMDB のインストールの詳細については，『HP Universal CMDB デプロイメント・ガイド（PDF)』を参照してください。

6 UCMDB のインストールとポスト・インストールの処理が完了したら，Configuration Manager Post Installation Configuration ウィザードが自動的に開始します。

7 ［Welcome］ページで［**Next**］をクリックすると，［Database Connection Configuration］ページが開きます。

8 データベース・タイプ（Oracle または Microsoft SQL Server）を選択し，ユーザ名とパスワードを入力します。［**Test**］ボタンをクリックして，接続を確認することをお勧めします。接続テストに問題がなければ，［**Next**］をクリックします。［Application Server Configuration］ページが開きます。

注：ウィザードが完了したら，さらに詳細なデータベース接続オプションを指定できます。詳細については，15ページ「詳細なデータベース接続オプションの構成」を参照してください。

---

9 ホスト名を入力して［**Next**］をクリックすると，［Windows Service Configuration］ページが開きます。

10 Configuration Manager を Windows サービスとしてインストールする場合は，チェック・ボックスを選択します。［**Next**］をクリックすると［Users Credentials］ページが開きます。

11 管理権限を持つユーザと統合権限を持つユーザについて，ユーザ名とパスワードを入力します。［**Next**］をクリックすると，［HP UCMDB Connection Configuration］ページが開きます。

12 使用中のコンピュータまたは別のコンピュータに UCMDB がすでにインストールされている場合は，UCMDB サーバが稼働中であることを確認してから作業を続行してください。

別のコンピュータに UCMDB をインストールする場合は，チェック・ボックスが選択されていることを確認し，必要なパラメータを入力してください。［**Test**］ボタンをクリックして，接続を確認することをお勧めします。接続テストに問題がなければ，［**Next**］をクリックします。［Post Installation Actions Summary］ページが開きます。

13 表示されている内容を確認します。誤りがなければ，［**Next**］をクリックします。ポスト・インストールが開始されます。

14 ［Finish］ページで［**Finish**］をクリックすると，ポスト・インストールが完了します。

15 UCMDB を初めて起動する場合を除き，UCMDB の列サイズを変更する必要があります。次の手順を実行してください。

a ［**マネージャ管理**］＞［**インフラストラクチャ設定マネージャ**］を選択します。［**オブジェクト ルート**］を［**data**］に変更します。UCMDB からログアウトした後で再度ログインすると，変更内容が有効になります。

b ［**マネージャ モデリング**］＞［**CI タイプ マネージャ**］を選択します。ツリー内で CI タイプの［**Data**］を選択し，［属性］タブを選択します。［**user label**］属性の［**値のサイズ**］を「900」に変更します。

c ［**インフラストラクチャ設定マネージャ**］に戻り，［**オブジェクト ルート**］設定を元の値に戻します。ログアウトした後で再度ログインすると，変更内容が有効になります。

16 データ・フロー管理が UCMDB 上ですでに稼働している場合，履歴データが破損している可能性があります。この問題を解決するには，次の手順を実行してください。

a Web ブラウザを起動し，アドレスに http://＜UCMDB サーバ・アドレス＞.＜ドメイン名＞:8080/jmx-console と入力します。

JMX コンソールの認証資格情報を入力します。デフォルトは次のとおりです。

➤ ログイン名 = **sysadmin**

➤ パスワード = **sysadmin**

b ［**UCMDB**］にある［**History DB Services**］を選択します。

c ［**Fix902EndTimeRecords**］メソッドを選択します。

d 実際のステータスの顧客の顧客 ID として「**1**」を入力し，［**Invoke**］をクリックします。

e 呼び出しに成功すると，「History DB is updated successfully」というメッセージが表示されます。

f 認証済みのステータスの顧客の顧客 ID として「**100001**」を入力し，［**Invoke**］をクリックします。

g 呼び出しに成功すると，「History DB is updated successfully」というメッセージが表示されます。

詳細なデータベース接続オプションの構成

データベースのデプロイメントで，さらに詳細なデータベース接続プロパティの設定が必要な場合は，Post Installation ウィザードの完了後にオプションを設定できます。Configuration Manager では，ベンダが提供する JDBC ドライバでサポートされるデータベース接続をすべて使用でき，データベース接続 URL を使った構成が可能です。詳細な接続オプションを構成するには，**＜Configuration Manager インストール・ディレクトリ＞¥conf¥database.properties** ファイルにある **jdbc.url** プロパティを編集します。

次に，Microsoft SQL Server での詳細オプションの設定例を示します。

- **Windows（NTLM）認証**：Windows 認証を適用するには，database.properties ファイルで JTDS 接続 URL にドメイン・プロパティを追加します。認証対象となる Windows ドメインを指定します。

  次に例を示します。

  ```
  jdbc:jtds:sqlserver://myServer:1433/
  myDatabase;sendStringParametersAsUnicode=false;domain=myDomain
  ```

- **SSL**：SSL を使用した MS SQL Server 接続のセキュリティについては，http://jtds.sourceforge.net/faq.html（英語サイト）を参照してください。

次に，Oracle Database Server での詳細オプションの設定例を示します。

- **Oracle URL**：Oracle ネイティブ・ドライバの接続 URL を指定します。有効な Oracle サーバ名と SID を指定します。また，**Oracle RAC** を使用している場合には，Oracle RAC 構成情報を指定してください。

注：ネイティブの Oracle JDBC URL の形式については，http://www.orafaq.com/wiki/JDBC#Thin_driver（英語サイト）を参照してください。Oracle RAC の URL の設定については，http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm（英語サイト）を参照してください。

- **SSL**：SSL を使用した Oracle 接続のセキュリティについては，次を参照してください。
  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604（英語サイト）
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6（英語サイト）

データベース構成 - MLU（多言語ユニット）のサポート

ここでは，ローカライズのサポートに必要なデータベース設定を説明します。

Oracle Server の設定

次の表は，Oracle Server で必要な設定を示します。

オプション	サポートされる設定	推奨	備考
文字セット	WE8ISO8859P1，UTF8，AL32UTF8	AL32UTF8	

Microsoft SQL Server の設定

次の表は，Microsoft SQL Server で必要な設定を示します。

オプション	サポートされる設定	推奨	備考
照合順序	大文字と小文字の区別：バイナリ並び替え順と大文字と小文字の区別はサポートされていません。大文字と小文字の区別は，アクセント，かな，文字幅を組み合わせた並び替え順のみがサポートされています。	照合順序は，[照合順序の設定] ダイアログ・ボックスで選択します。バイナリのチェック・ボックスは選択しないでください。アクセント，かな，文字幅の区別は，各データ言語の要件に従って選択します。OS Windows の地域設定の言語と同じ言語を選択してください。	[照合順序] のロケールと英語のデフォルト設定に限定。
照合順序データベースのプロパティ	サーバのデフォルト		

注：

すべての言語共通：**＜言語＞_CI_AS** は，最低限必要なオプションです。
日本語で「かなを区別する」オプションと「文字幅を区別する」オプションを選択する場合には，**Japanese_CI_AS_KS_WS** または **Japanese_90_CI_AS_KS_WS** を推奨します。この設定は，日本語の文字はアクセントを区別，かなを区別，文字幅を区別することを示しています。

- **アクセントを区別する（_AS）:** アクセント付き文字とアクセントなし文字を区別します。たとえば，**a** と **á** は区別されます。このオプションを選択しないと，Microsoft SQL Server では，アクセント付きの文字とアクセントなしの文字が同一とみなされます。
- **かなを区別する（_KS）:** 日本語のひらがなとカタカナを区別します。このオプションを選択しないと，Microsoft SQL Server では，ひらがなとカタカナが同一とみなされます。
- **文字幅を区別する（_WS）:** 半角文字と全角文字を区別します。このオプションを選択しないと，Microsoft SQL Server では，半角文字と全角文字が同一とみなされます。

Lightweight シングル・サインオン（LW-SSO）の有効化

Configuration Manager ユーザの中には，UCMDB へのログインが許可されているユーザがいます。Configuration Manager では，このようなユーザ向けに UCMDB に直接リンクできるユーザ・インタフェースが用意されています（[**管理**] > [**UCMDB を開く**] を選択）。シングル・サインオン（Configuration Manager へのログイン後，UCMDB へのログインを不要にする機能）を使用するには，Configuration Manager と UCMDB の両方で LW-SSO を有効にし，同じ initString を使用するように設定します。このタスクでは，Configuration Manager と UCMDB でLW-SSO を有効にする方法を説明します。

LW-SSO を有効にするには，次の手順を実行します。

1 Configuration Manager インストール・ディレクトリにある **¥servers¥server-0¥webapps¥cnc¥WEB-INF¥classes¥cnclwssofmconf.xml** ファイルを開きます。

注：Configuration Manager を起動しないと，このファイルは作成されません。

---

2 次のセクションを探します。

```
enableLWSSO enableLWSSOFramework="true"
```

値が「**true**」に設定されていることを確認します。

3 次のセクションを探します。

```
lwssoValidation  id="ID000001">
<domain> </domain>
```

<domain> の後に，Configuration Manager サーバ・ドメインを入力します。

4 次のセクションを探します。

```
<initString="この文字列を置換"></crypto>
```

"この文字列を置換" の部分を，LW-SSO で統合するすべての信頼済みアプリケーションが共有する文字列に置き換えます。

5 次のセクションを探します。

```
<!--multiDomain>
<trustedHosts>
<DNSDomain>アプリケーション・ドメインで置換</DNSDomain>
<DNSDomain>ドメインまたは他のアプリケーションで置換</DNSDomain>
<trustedHosts>
</multiDomain-->
```

先頭のコメント文字を削除して，DNSDomain 要素に Configuration Manager サーバ・ドメインを入力します（**アプリケーション・ドメインで置換**の部分を置き換えます）。手順 3（18ページ）で入力したサーバ・ドメインを指定してください。

6 変更したファイルを保存し，サーバを再起動します。

7 Web ブラウザを起動し，アドレスに http://＜UCMDB **サーバ・アドレス**＞.＜**ドメイン名**＞:8080/jmx-console と入力します。

JMX コンソールの認証資格情報を入力します。デフォルトは次のとおりです。

- ログイン名 = **sysadmin**
- パスワード = **sysadmin**

8 ［**UCMDB-UI**］の下にある［**name=LW-SSO configuration**］をクリックすると，［JMX MBEAN View］ページが開きます。

9 ［**setEnabledForUI**］メソッドを選択し，値を「**true**」に指定して，［**Invoke**］をクリックします。

10 ［**setDomain**］メソッドを選択します。UCMDB サーバのドメイン名を入力し，［**Invoke**］をクリックします。

11 ［**setInitString**］メソッドを選択します。手順 4（18ページ）で，Configuration Manager で指定した initString を入力し，［**Invoke**］をクリックします。

12 Configuration Manager と UCMDB が別のドメインにある場合は，［**addTrustedDomains**］メソッドを選択し，UCMDB と Configuration Manager の各サーバのドメイン名を入力します。［**Invoke**］をクリックします。

13 設定メカニズムで保存されている LW-SSO 構成をそのまま表示するには，［**retrieveConfigurationFromSettings**］メソッドを選択して［**Invoke**］をクリックします。

14 実際に読み込まれた LW-SSO 構成を表示するには，［**retrieveConfiguration**］メソッドを選択して［**Invoke**］をクリックします。

IPv6 のサポート

Configuration Manager は，顧客向け URL のみで IPv6 URL をサポートします。

Configuration Manager で IPv6 アドレスを使用するには，次の手順を実行します。

1 使用中のオペレーティング・システムが IPv6 をサポートしていることを確認します。詳細については，オペレーティング・システムのマニュアルを参照してください。

2 **＜Configuration Manager インストール・ディレクトリ＞**の **conf** ディレクトリにある **client-config.properties** ファイルを開きます。**bsf.server.url** パラメータの値に，角括弧で囲んだ IPv6 アドレスを指定します。次に例を示します。

```
bsf.server.url=http://[2620:0:a17:e008:d840:5b0f:2040:519c]:8080/bsf
```

第 2 章

Configuration Manager Post Installation Configuration ウィザード

本章の内容

Configuration Manager のポスト・インストール構成の概要

本章では，Configuration Manager Post Installation ウィザードのページと，各ページで実行する構成タスクについて詳しく説明します。本章の内容は，ウィザード・ページで［**ヘルプ**］をクリックしても参照できます。

［Database Connection］ページ

本項の内容

概要

標準 URL 接続に関連するデータベース接続を設定する必要があります。さらに高度な機能（Oracle Real Application Cluster など）が必要な場合は，標準接続を設定してから，使用する機能に合わせて **database.properties** ファイルを手作業で編集してください。

Configuration Manager は，Oracle および Microsoft SQLServer で提供されているネイティブ・ドライバを使用します。したがって，一般的に，データベース URL で設定可能なネイティブ・ドライバ機能はすべてサポートされます。URL は **database.properties** ファイルで記述されています。

注：より高度な機能を使用する場合の設定は，ポスト・インストール作業と構成が完了してから行ってください。

パラメータ

データベース接続の設定では，次のパラメータを定義します。

パラメータ	推奨値	説明
Vendor	＜ユーザ定義＞	データベース・ベンダ 設定可能な値：**Oracle** または **Microsoft** HP Universal CMDB のインストールには, Configuration Manager と同じインストーラまたは異なるインストーラを使用できます。 Configuration Manager と UCMDB を同じマシンに同じインストーラを使用してインストールする場合，このパラメータのデフォルト値は，UCMDB の Post Installation ウィザードで選択したデータベース・ベンダになります。 デフォルト値が設定されるのは，同じインストーラを使って両方のアプリケーションをインストールする場合のみです。異なるインストール・パッケージを使用する場合は，UCMDB と Configuration Manager を同じマシン上にインストールしても，Post Installation ウィザードでデフォルト値は表示されません。
Hostname	＜ユーザ定義＞	データベース・サーバのホスト名 Configuration Manager と UCMDB を同じマシンに同じインストーラを使用してインストールする場合，このパラメータのデフォルト値は，UCMDB の Post Installation ウィザードで選択したデータベース・サーバになります。 **この値は必須です。**

パラメータ	推奨値	説明
Port	＜ユーザ定義＞	データベース・リスナのポート Configuration Manager と UCMDB を同じマシンに同じインストーラを使用してインストールする場合，このパラメータのデフォルト値は，UCMDB の Post Installation ウィザードで選択したデータベース・ポートになります。 Oracle でのデフォルト値は **1521** です。 Microsoft SQL Server でのデフォルト値は **1433** です。 **この値は必須です。**
SID/DB	＜ユーザ定義＞	Oracle SID の名前，またはMicrosoft SQL Server データベースの名前 Configuration Manager と UCMDB を同じマシンに同じインストーラを使用してインストールする場合，このパラメータのデフォルト値は，UCMDB の Post Installation ウィザードで選択したデータベース SID/DB になります。 **この値は必須です。**
Username	＜ユーザ定義＞	データベースへのログインに使用するユーザ名 **この値は必須です。**
Password	＜ユーザ定義＞	データベースへのログインに使用するパスワード

オプション

次のオプションを選択できます。

パラメータ	推奨値	説明
Encrypt password	＜ユーザ定義＞	このオプションを選択すると，**database.properties** ファイル内のパスワードが暗号化されます。テキスト・ファイルにパスワードを格納している場合は，セキュリティ強化のために暗号化をお勧めします。
Create schema objects	＜ユーザ定義＞	このオプションを選択すると，Configuration Manager の実行に必要なスキーマ・オブジェクトが作成されます。Configuration Manager オブジェクトで設定されている既存のスキーマを使用する場合のみ，このオプションの選択を解除してください。

テスト

注：接続プロパティをテストしてから作業を続行することを強くお勧めします。

接続プロパティをテストするには，［**Test**］をクリックします。ウィザードが起動し，データベースにアクセスして接続を確認します。［**Test**］ボタンの右側にテスト結果が表示されます。

データベースでは，さまざまなエラー・メッセージが表示されます。入力したユーザ名やパスワードに誤りがあるなど，わかりやすいメッセージが表示されます。エラーを修正してテスト結果に問題がないことを確認してから，作業を続行してください。

［Application Server］ページ

本項の内容

概要

次で示すデフォルトのポート番号を使って Configuration Manager アプリケーション・サーバを設定します。

パラメータ

Configuration Manager アプリケーション・サーバの設定では，次のパラメータを定義します。

パラメータ	推奨値	説明
Hostname	＜ユーザ定義＞	アプリケーション・サーバの外部名 デフォルトは，ウィザード（および Configuration Manager）を実行しているコンピュータの完全修飾ホスト名です。ただし，別の名前を指定する場合もあります（Configuration Manager アプリケーション・サーバの前面に Web サーバをデプロイする場合など）。
Customize ports	＜ユーザ定義＞	デフォルトでは，このオプションは選択されません。選択すると，アプリケーション・サーバのデフォルトのポート番号をカスタマイズできます。

パラメータ	推奨値	説明
HTTP port	＜ユーザ定義＞	Configuration Manager アプリケーション・サーバの HTTP ポート デフォルト値：**8080** HP Universal CMDB と同じマシンにインストールした場合のデフォルト値：**8180**
HTTP port	＜ユーザ定義＞	Configuration Manager アプリケーション・サーバの HTTPS ポート デフォルト値：**8443** UCMDB と同じコンピュータにインストールした場合のデフォルト値：**8143**
Tomcat port	＜ユーザ定義＞	Configuration Manager アプリケーション・サーバの管理ポート デフォルト値：**8005**
AJP port	＜ユーザ定義＞	Configuration Manager アプリケーション・サーバの AJP（Apache Java Protocol）ポート デフォルト値：**8009**
JMX HTTP port	＜ユーザ定義＞	Configuration Manager アプリケーション・サーバの JMX HTTP ポート デフォルト値：**39900**
JMX remote port	＜ユーザ定義＞	Configuration Manager アプリケーション・サーバの JMX リモート・ポート デフォルト値：**39600**

［Windows Service Configuration］ページ

Configuration Manager を Windows サービスとしてインストールするかどうかを選択します。このオプションを選択できるのは，Windows マシンにインストールする場合のみです。

Windows サービスは，**cnc-home/bin** ディレクトリの **create-windows-service.bat** ユーティリティを使用して手動で設定できます。

［Users Credentials］ページ

本項の内容

➤ 28 ページ「概要」

概要

次に示す Configuration Manager の初期ユーザを設定します。

パラメータ	推奨値	説明
Admin user	＜ユーザ定義＞	Configuration Manager の管理ユーザである「スーパー・ユーザ」
Integration user	＜ユーザ定義＞	統合の目的で HP Universal CMDB に Configuration Manager が作成するユーザ

注：資格情報として，管理ユーザとインテグレーション・ユーザが使用するユーザ名とパスワードが必要です。

［HP Universal CMDB Connection］ページ

本項の内容

➤ 28 ページ「概要」

➤ 29 ページ「パラメータ」

➤ 30 ページ「テスト」

概要

HP Universal CMDB への接続の設定はオプションです。

UCMDB と同じマシンに Configuration Manager を一緒にインストールする場合は，このページでの入力は不要です。

UCMDB を一緒にインストールしない場合, UCMDB を別のマシンにインストールする場合（localhost 上の UCMDB に接続する場合を含む），Configuration Manager の前に UCMDB をインストールする場合には，UCMDB を稼働状態にし，接続プロパティを指定する必要があります。

注：UCMDB のリモート・インスタンスを使ってインストールする場合，このインスタンスを稼働状態にする必要があります。Configuration Manager と UCMDB を同じマシンにインストールする場合は，UCMDB をシャットダウンした状態でウィザードを実行してください。

パラメータ

UCMDB 接続の設定では，次のパラメータを定義します。

パラメータ	推奨値	説明
Use HP UCMDB on a different host	＜ユーザ定義＞	Configuration Manager と UCMDB を別のマシンにインストールする場合，このオプションを選択すると，他のプロパティがすべて有効になります。
Hostname	＜ユーザ定義＞	UCMDB がインストールされているホスト名
Port	＜ユーザ定義＞	UCMDB がリッスンするポート
Protocol	＜ユーザ定義＞	HTTP または HTTPS
Customer	＜ユーザ定義＞	UCMDB 顧客
Administrative username	＜ユーザ定義＞	UCMDB sysadmin のユーザ名
Administrative password	＜ユーザ定義＞	UCMDB sysadmin のパスワード

テスト

注：接続プロパティをテストしてから作業を続行することを強くお勧めします。

接続プロパティをテストするには，［**Test**］をクリックします。ウィザードが起動し，UCMDB にアクセスして接続を確認します。［**Test**］ボタンの右側にテスト結果が表示されます。

UCMDB では，さまざまなエラー・メッセージが表示されます。入力したユーザ名やパスワードに誤りがあるなど，わかりやすいメッセージが表示されます。エラーを修正してテスト結果に問題がないことを確認してから，作業を続行してください。

［Summary］ページ

ウィザード・ページでこれまでに選択した内容がすべて表示されます。内容がすべて正しいことを確認し，必要に応じて変更します。内容が正しいことを確認したら，［**Next**］をクリックします。ウィザードは，構成タスクを完了します。

［Finish］ページ

Configuration Manager Post Installation Configuration ウィザードの最後のページです。これで，ポスト・インストール構成タスクは完了です。［**Finish**］をクリックすると，ウィザードが終了します。

注：すべてのタスクが問題なく完了している場合でも，**cnc-home/tmp/chp/app.log** のログをチェックすることをお勧めします。

第 3 章

LDAP の構成

HP UCMDB Configuration Manager は，LDAP を使用してユーザ，役割，権限を管理します。本章では，LDAP の構成とトラブルシューティングの手順を説明します。

本章の内容

LDAP の概要

Configuration Manager には，内部 LDAP サーバ（ユーザ・インタフェースでは「**SHARED**」と認識）が付属します。また，ユーザ組織で使用している LDAP サーバへの接続も可能です。Configuration Manager は，このような LDAP サーバを使用してユーザ，グループ，役割の検索，カスタマイズ・データの格納，ユーザ認証を行います。このような情報は，組織の LDAP サーバと内部 LDAP サーバに分けて管理することができます。

内部（共有）LDAP サーバに役割を格納し，それ以外の情報を外部（組織）LDAP サーバに格納する方法が一般的です。

プロバイダの選択

1 **Configuration Manager** に管理者ユーザでログインします。

2 ［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］を選択し，各プロバイダで［SHARED］または［EXTERNAL］を選択します（デフォルトは［SHARED］です）。

- 認証プロバイダ
- グループ・プロバイダ
- カスタマイズ・プロバイダ
- 役割プロバイダ
- 役割関係プロバイダ

3 構成セットを保存します。

組織 LDAP への接続

HP UCMDB Configuration Manager では，初期設定として内部（共有）LDAP が構成されます。ここでは，組織 LDAP サーバに接続する手順を説明します。

本項の内容

LDAP 接続の構成

ここでは，Configuration Manager を外部 LDAP サーバに接続する方法を説明します。外部 LDAP サーバは組織 LDAP であり，組織のユーザが格納されています。

1 **Configuration Manager** に管理者ユーザでログインします。

2 ［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］＞［**外部ユーザ リポジトリ**］を選択し，組織 LDAP のプロパティに従って次の属性を変更します。

General LDAP connection

ldapHost：＜LDAP ホスト名＞

ldapPort：＜LDAP ポート番号＞

enableSSL：＜LDAP への接続に SSL を使用するかどうか（true または false）＞

useAdministrator：＜LDAP への接続に使用するユーザ（true または false）＞

ldapAdministrator：＜LDAP ユーザ名（**useAdministrator=true** の場合に定義＞

ldapAdministratorPassword：＜LDAP ユーザ・パスワード（**useAdministrator=true**）の場合に定義）＞

3 構成セットを保存します。

グループ・プロバイダとユーザ・プロバイダの構成

ここでは，グループとユーザのプロバイダとして組織 LDAP（外部リポジトリ）を設定する手順を説明します。この構成を行うと，認証には内部 LDAP（共有リポジトリ）を使用しますが，ユーザとグループは外部 LDAP から取得されます。外部 LDAP の構成のテストや，組織ユーザに権限を割り当てる際に使用します。

グループ・プロバイダとユーザ・プロバイダを設定するには，次の手順を実行します。

1 このページが開いていない場合は，［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］＞［**外部ユーザ リポジトリ**］を選択します。この作業では，33ページ「LDAP 接続の構成」で保存したドラフトの構成セットを使用してください。

2 組織 LDAP のプロパティに従って，次の属性を変更します。

a **Users search**

usersBase：＜ユーザ検索で使用するベース DN＞

usersScope：＜ユーザ検索で使用するスコープ＞

usersFilter：＜ユーザ検索で使用するフィルタ＞

b **Users object class**（LDAP のベンダによって異なります）

usersObjectClass：＜ユーザの LDAP オブジェクト・クラス＞

usersUniquelDAttribute：＜ユーザの一意の ID を示す LDAP 属性＞

次の属性はオプションです。

usersDisplayNameAttribute：＜ユーザの表示名を示す LDAP 属性＞

usersLoginNameAttribute：＜ユーザのログイン名を示す LDAP 属性＞

usersFirstNameAttribute：＜ユーザの名を示す LDAP 属性＞

usersLastNameAttribute：＜ユーザの姓を示す LDAP 属性＞

usersEmailAttribute：＜ユーザの電子メールを示す LDAP 属性＞

usersPreferredLanguageAttribute：＜ユーザの優先言語を示す LDAP 属性＞

usersPreferredLocationAttribute：＜ユーザの優先場所を示す LDAP 属性＞

usersTimeZoneAttribute：＜ユーザのタイム・ゾーンを示す LDAP 属性＞

usersDateFormatAttribute：＜ユーザの日付形式を示す LDAP 属性＞

usersNumberFormatAttribute：＜ユーザの数値形式を示す LDAP 属性＞

usersWorkWeekAttribute：＜ユーザの就業曜日を示す LDAP 属性＞

usersTenantIDAttribute：＜ユーザのテナント ID を示す LDAP 属性＞

usersPasswordAttribute：＜ユーザのパスワードを示す LDAP 属性＞

c Groups search

groupsBase：＜グループ検索で使用するベース DN＞

groupsScope：＜グループ検索で使用する LDAP スコープ＞

groupsFilter：＜グループ検索で使用するフィルタ＞

rootGroupsBase：＜ルート・グループ検索で使用するベース DN＞

rootGroupsScope：＜ルート・グループ検索で使用する LDAP スコープ＞

rootGroupsFilter：＜グループ検索で使用するフィルタ＞

d Groups object class（LDAP のベンダによって異なります）

groupsObjectClass：＜グループの LDAP オブジェクト・クラス＞

groupsMembersAttribute：＜グループ・メンバの LDAP 属性＞

次の属性はオプションです。

groupsNameAttribute：＜グループの一意の名前を示す LDAP 属性＞

groupsDisplayNameAttribute：＜グループの表示名を示す LDAP 属性＞

groupsDescriptionAttribute：＜グループの説明を示す LDAP 属性＞

enableDynamicGroups：＜動的グループを有効化＞

dynamicGroupsClass：＜動的グループの LDAP オブジェクト・クラス＞

dynamicGroupsMemberAttribute：＜動的グループ・メンバの LDAP 属性＞

dynamicGroupsNameAttribute：＜動的グループの一意の名前を示す LDAP 属性＞

dynamicGroupsDisplayNameAttribute：＜動的グループの表示名を示す LDAP 属性＞

dynamicGroupsDescriptionAttribute：＜動的グループの説明を示す LDAP 属性＞

e Groups hierarchy（組織 LDAP でグループ階層を使用する場合）

enableNestedGroups：＜ネストされたグループのサポートを有効化＞

maximalAllowedGroupsHierarchyDepth：＜グループ階層で許容される深さの最大値＞

f Advanced configuration

ldapVersion：＜LDAP バージョン＞

baseDistinguishNameDelimiter：＜ベース DN の区切り文字＞

scopeDelimiter：＜スコープの区切り文字＞

attributeValuesDelimiter：＜LDAP 属性値の区切り文字＞

3 構成セットのドラフトを保存します。

構成セットのアクティブ化

1［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］を選択し，次のように変更します。

［外部 UUM ソース］：True

［グループ プロバイダ］：EXTERNAL

［ユーザ プロバイダ］：EXTERNAL

2 構成セットを保存し，アクティブ化します。

3 Configuration Manager サーバからログオフし，再起動します。

ユーザ権限の割り当て

ここでは，**システム管理者**の役割を組織ユーザ（1 人または複数）に割り当てる手順を説明します。**システム管理者**の役割を割り当てられたユーザは，他の組織ユーザに役割を割り当てることができるようになります。

1 Configuration Manager に管理者ユーザでログインします。

2 ユーザ管理モジュールを開きます（［**管理**］＞［**ユーザ管理**］を選択します）。

3 組織 LDAP に格納されているグループとユーザが表示されます。

4［**ユーザ管理**］＞［**ユーザの検索**］表示枠を選択し，システム管理者となるユーザを検索します（例：［名］に j*，［姓］に Smith を指定）。

5［**システム管理者**］の役割をユーザに追加します。

認証プロバイダを外部 LDAP に設定

ここでは，認証プロバイダを外部の組織 LDAP に設定する手順を説明します。これにより，認証に組織ユーザが使用されます。

1 ［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］を選択し，次のように変更します。

認証プロバイダ：EXTERNAL

2 構成セットを保存し，アクティブ化します。

3 **Configuration Manager** サーバからログオフし，再起動します。

4 **システム管理者**の役割を持つ組織ユーザでログインします。

LDAP 証明書のインポート

組織 LDAP への接続時に証明書が必要な場合は，次の手順を実行します。

1 証明書をファイルにエクスポートします。

2 Configuration Manager Windows サービスを停止します。

3 次のコマンドを実行します。

＜Configuration Manager インストール・ディレクトリ＞¥java¥windows¥x86_64¥bin¥keytool.exe -import -trustcacerts -alias ＜証明書エイリアス＞ -keystore ＜Configuration Manager インストール・ディレクトリ＞¥java¥windows¥x86_64¥lib¥security¥cacerts -storepass changeit -file ＜証明書のファイル・パス＞

4 Configuration Manager Windows サービスを開始します。

内部（共有）LDAP の構成

内部（共有）LDAP サーバのパスワードの変更（オプション）

セキュリティ強化のために，内部（共有）LDAP サーバのパスワードを変更することができます。

1 **HP Universal CMDB Configuration Manager** にログインします。

2 コマンド・ラインを開き，**＜Configuration Manager インストール・ディレクトリ＞¥ldap¥serverRoot¥bat** フォルダに移動します。

3 **ldappasswordmodify -h localhost -p ＜LDAP ポート＞ -D "cn=Directory Manager" -w ＜LDAP 管理パスワード＞ -c ＜LDAP 管理パスワード＞ -n ＜新しい LDAP 管理パスワード＞** を実行します。

   a LDAP 管理パスワードのデフォルト値は **ldapadmin** です。

   b デフォルト・ポートは **2389** です。

   c コマンドが問題なく完了したことを確認し，次の手順に進みます。

4 **UCMDB Configuration Manager** で，［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］＞［**共有ユーザ リポジトリ**］を選択します。

5 **ldapAdministratorPassword** 属性で指定されているパスワードを変更します。

6 構成セットを保存し，アクティブ化します。

7 **UCMDB Configuration Manager** からログオフします。

8 **UCMDBConfiguration Manager** サーバを再起動します。

内部（共有）LDAP ポートの構成

デフォルト・ポートは 2389 ですが，他のアプリケーションがすでに使用している可能性があります。このような場合は，次の手順でデフォルト・ポートを変更します。

内部 LDAP ポートを構成するには，次の手順を実行します。

1 コマンド・ラインを開き，**＜Configuration Manager インストール・ディレクトリ＞¥ldap¥serverRoot¥bat** フォルダに移動します。

2 次のコマンドを実行します。
dsconfig -h localhost -p 2444 -D "cn=directory manager" -w ＜LDAP 管理パスワード＞ --trustAll -X -n set-connection-handler-prop --handler-name "LDAP Connection Handler" --set listen-port:＜新しいポート＞

＜LDAP 管理パスワード＞のデフォルト値は **ldapadmin** です。

3 エラー・メッセージが表示されないことを確認してから，次の手順に進みます。

4 HP Universal CMDB Configuration Manager にログインします。

5 UCMDB Configuration Manager で，［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］＞［**共有ユーザ リポジトリ**］を選択し，**ldapPort** 属性で指定されているポート番号を変更します。

6 構成セットを保存し，アクティブ化します。

7 UCMDB Configuration Manager からログオフします。

8 UCMDB Configuration Manager サーバを再起動します。

LDAP のトラブルシューティング

問題：LDAP サーバとの接続を確立できません。通信例外がログに記録されます。

解決策：LDAP ホスト，ポート，SSL モードの設定を確認します。

a LDAP ホストとポートの設定が正しいことを確認します。［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］＞［**外部ユーザ リポジトリ**］を選択し，**ldapHost** と **ldapPort** の設定を確認します。

b SSL モードの設定が正しいことを確認します。組織 LDAP の管理者に，LDAP 接続には管理者ユーザを使用する必要があるかどうかを確認します。［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］＞［**外部ユーザ リポジトリ**］を選択し，**enableSSL** の設定を確認します。

c 適切なサーバ証明書がインストールされていることを確認します。次のコマンドを実行します。

＜Configuration Manager インストール・ディレクトリ＞¥java¥windows¥x86_64¥bin¥keytool.exe -list -trustcacerts [-alias ＜証明書エイリアス＞] -keystore ＜Configuration Manager インストール・ディレクトリ＞¥java¥windows¥x86_64¥lib¥security¥cacerts -storepass changeit

d 組織 LDAP の管理者に, LDAP 接続には管理者ユーザを使用する必要があるかどうかを確認します。［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］＞［**外部ユーザ リポジトリ**］を選択し，次の設定を確認します。**useAdministrator**，**ldapAdministrator**，**ldapAdministratorPassword**

問題：ユーザ管理またはグループ管理の画面にグループが表示されません。ログに例外は記録されていません。

解決策：次の内容を確認します。

a ユーザとグループの検索フィルタの設定が正しいことを確認します。［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］＞［**外部ユーザ リポジトリ**］を選択し，次のプロパティを変更します。**usersBase**，**usersScope**，**usersFilter**，**groupsBase**，**groupsScope**，**groupsFilter**，**rootGroupsBase**，**rootGroupsScope**，**rootGroupsFilter**

b LDAP クライアントのブラウザを開き，ベース DNS にユーザが表示されることを確認します。

問題：UI の処理速度が極端に低下します。

解決策：一般的に，処理速度の低下は，LDAP で構成したグループやユーザの数が多すぎることが原因です。次の手順に従ってベース DNS とフィルタを構成し，サブセットに分けることでグループの数を減らします。

a ［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］＞［**外部ユーザ リポジトリ**］を選択します。

b 次の設定を変更します。**usersBase**，**usersScope**，**usersFilter**，**groupsBase**，**groupsScope**，**groupsFilter**，**rootGroupsBase**，**rootGroupsScope**，**rootGroupsFilter**

問題：ユーザが存在するにも関わらず，ユーザ管理またはグループ管理の画面に表示されません。

解決策：ユーザとグループの管理画面には，グループに所属しているユーザのみが表示されます。メイン画面でユーザを表示するためには，ユーザを LDAP のグループに割り当てる必要があります。

問題：ログインに時間がかかります。

解決策：そのユーザは，多数のグループに所属していると考えられます。グループ検索フィルタを変更してグループの数を少なくすると，起動時間を短縮できます。

a ［**管理**］＞［**サーバ管理**］＞［**ユーザ管理**］＞［**ユーザ管理の構成**］＞［**外部ユーザ リポジトリ**］を選択します。

b **groupsFilter** の設定を変更します。

第 4 章

Lightweight シングル・サインオン認証（LW-SSO）のリファレンス

本章の内容

LW-SSO 認証の概要

LW-SSO とは，アクセス制御方法の 1 つであり，一度ログインしたユーザは，再びログインしなくても複数のソフトウェア・システムのリソースにアクセスできるようになります。構成されたソフトウェア・システム・グループ内のアリケーションは認証を信頼するので，アプリケーション間を移動する際に追加で認証を行う必要はありません。

ここでは，LW-SSO バージョン 2.2 および 2.3 に関する内容を説明します。

本項の内容

LW-SSO トークンの期限

LW-SSO トークンの期限に基づいて，アプリケーションのセッションの期限が決まります。したがって，トークンの期限は，アプリケーションのセッション期限またはそれよりも後にする必要があります。

LW-SSO トークンの期限の推奨値

LW-SSO を使用するアプリケーションごとに，トークンの期限を設定する必要があります。推奨値は 60 分です。高度なセキュリティを必要としないアプリケーションでは，300 分に設定することも可能です。

GMT 時間

LW-SSO に参加するアプリケーションはすべて同じ GMT 時間を使用し，誤差が 15 分以内になるように調整してください。

マルチドメイン機能

マルチドメイン機能では，LW-SSO に参加するアプリケーションを，異なる DNS ドメインのアプリケーションと統合する場合，すべてのアプリケーションで trustedHosts 設定（または **protectedDomains** 設定）を行う必要があります。さらに，**lwsso** 要素に正しいドメインを追加する必要があります。

URL 機能で使用する SecurityToken の取得

他のアプリケーションが **URL の SecurityToken** として送信した情報を受信するには，ホスト・アプリケーション設定の **lwsso** 要素で正しいドメインを設定する必要があります。

LW-SSO のセキュリティに関する警告

ここでは，LW-SSO 設定に関するセキュリティ上の警告について説明します。

➤ **LW-SSO の InitString 機密パラメータ**：LW-SSO では，対称暗号化方式を使用して LW-SSO トークンを検証および生成します。構成した **initString** パラメータは，秘密キーの初期化に使用されます。アプリケーションがトークンを生成すると，同じ initString パラメータを使用する各アプリケーションがトークンを検証します。

注意：

➤ **initString** パラメータを設定しないと，LW-SSO は使用できません。

➤ **initString** パラメータは機密情報なので，公開や転送は慎重に行い，永続性を考慮して取り扱ってください。

➤ **initString** パラメータの共有は，LW-SSO を使用して相互に統合されたアプリケーション間のみに限定する必要があります。

➤ **initString** パラメータは，12 文字以上です。

➤ **必要な場合のみ LW-SSO を有効化**：LW-SSO は，必要な場合以外は無効にしてください。

➤ **認証セキュリティのレベル**：LW-SSO に参加するアプリケーションの中で最も弱い認証フレームワークを使用し，他の参加アプリケーションによって信頼されている LW-SSO トークンを発行するアプリケーションを基準に，アプリケーション全体の認証セキュリティ・レベルが決まります。

したがって，LW-SSO トークンの発行は，強力で安全な認証フレームワークを使用するアプリケーションに限定することをお勧めします。

- **対称暗号化方式による影響**：LW-SSO は，対称暗号化方式を使用して LW-SSO トークンを発行および検証します。LW-SSO を使用するアプリケーションによって発行されるトークンは，同じ **initString** パラメータを共有するすべてのアプリケーションによって信頼されることになります。したがって，initString を共有するアプリケーションが信頼されていない場所に配置されている場合や信頼されていない場所からアクセス可能な場合には，セキュリティ上のリスクが伴います。

- **ユーザのマッピング（同期）**：LW-SSO フレームワークでは，統合アプリケーション間のユーザ・マッピングは保証されません。したがって，統合アプリケーションではユーザ・マッピングを監視する必要があります。すべての統合アプリケーションで同じユーザ・レジストリ （LDAP/AD など）を共有することをお勧めします。

  ユーザのマッピングに失敗すると，セキュリティ違反が発生し，アプリケーションが予期しない動作をすることがあります。たとえば，実際には異なるユーザでも，複数のアプリケーションで同じユーザ名が割り当てられている可能性があります。

  また，ユーザがあるアプリケーション（AppA）にログインしてから，コンテナ認証またはアプリケーション認証を使用する別のアプリケーション（AppB）にアクセスする場合，ユーザのマッピングに失敗すると，ユーザは手動で AppB にログインしてユーザ名を入力しなければなりません。このとき，AppA へのログイン時とは別のユーザ名を入力し，AppA または AppB からさらに別のアプリケーション（AppC）にアクセスする場合，AppC へのログインには，AppA または AppB へのログインで使用したユーザ名がそのまま使用されます。

- **ID マネージャ**：認証に使用される機能です。ID マネージャ内にある保護されていないリソースはすべて，LW-SSO 構成ファイル内で **nonsecureURLs** に設定する必要があります。

トラブルシューティングおよび制限事項

既知の問題

ここでは，LW-SSO 認証に関する既知の問題について説明します。

➤ **セキュリティ・コンテキスト**：LW-SSO のセキュリティ・コンテキストでは，1 つの属性名につき 1 つの属性値のみがサポートされます。

したがって，SAML2 トークンが同じ属性名の値を複数送信しても，LW-SSO フレームワークは 1 つの値しか受信しません。

同様に，同じ属性名の値を複数送信するように IdM トークンが設定されていても，LW-SSO フレームワークで許可される値は 1 つのみです。

➤ **Internet Explorer 7 使用時のマルチドメインのログアウト機能**：次の場合，マルチドメインのログアウト機能は失敗することがあります。

➤ Internet Explorer 7 を使用していて，アプリケーションのログアウト手順で HTTP 302 リダイレクトの動作が 4 回以上連続で呼び出された場合。

この場合，Internet Explorer 7 では HTTP 302 リダイレクト応答が正しく処理されず，［**Internet Explorer ではこのページは表示できません**］というエラー・ページが表示されることがあります。

この問題を回避するには，アプリケーションのログアウト手順で実行するダイレクト・コマンドの回数を少なくすることを推奨します。

制限事項

LW-SSO 認証では，次の制限に注意してください。

➤ **アプリケーションへのクライアント・アクセス**

ドメインが LW-SSO 構成で定義されている場合

➤ アプリケーションのクライアントは，ログイン URL で FQDN（完全修飾ドメイン名）を使用してアプリケーションにアクセスする必要があります（http://myserver.**企業ドメイン名**.com/WebApp など）。

➤ LW-SSO では，IP アドレスを使用した URL はサポートされていません（http://192.168.12.13/WebApp など）。

➤ LW-SSO では，ドメイン指定のない URL はサポートされていません（http://myserver/WebApp など）。

LW-SSO 構成でドメインが定義されていない場合 : クライアントは，ログイン URL で FQDN が指定されていないアプリケーションにアクセスできます。この場合，このマシン専用に，ドメイン情報なしで LW-SSO のセッション Cookie が作成されます。この Cookie は他のブラウザに委譲されたり，同じ DNS ドメインにある別のコンピュータに渡されることはありません。したがって，LW-SSO は同じドメインで機能しなくなります。

- **LW-SSO フレームワークの統合 :** アプリケーションで LW-SSO 機能を使用するには，アプリケーションをあらかじめ LW-SSO フレームワーク内に統合しておく必要があります。
- **マルチドメインのサポート**
  - マルチドメイン機能は，HTTP リファラを使用します。したがって，LW-SSO ではアプリケーション間のリンクはサポートされていますが, 両方のアプリケーションが同じドメイン上にある場合を除き, ブラウザ・ウィンドウでの URL 入力はサポートされていません。
  - 最初のクロスドメイン・リンクには **HTTP POST** を使用できません。

    マルチドメイン機能では，最初に **HTTP POST** 要求を使用することはサポートされていません（**HTTP GET** 要求のみサポートされています)。たとえば，あるアプリケーションから別のアプリケーションへの HTTP リンクでは，**HTTP GET** 要求はサポートされていますが，**HTTP FORM** 要求はサポートされていません。2 回目以降の要求は，すべて **HTTP POST** か **HTTP GET** のいずれかになります。
  - LW-SSO トークンのサイズ

    LW-SSO が異なるドメインのアプリケーション間で転送できる情報量は，15 のグループ/役割/属性までに制限されています（各項目の長さは平均 15 文字です)。

- マルチドメイン・シナリオでの，保護されたページ（HTTPS）から保護されていないページ（HTTP）へのリンク

  保護されたページ（HTTPS）から保護されていないページ（HTTP）にリンクする場合，マルチドメインは機能しません。これはブラウザの制限事項の 1 つです。保護されたリソースから保護されていないリソースにリンクする際，リファラ・ヘッダは送信されません。具体例については，http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP（英語サイト）を参照してください。

- **SAML2 トークン**

  - SAML2 トークンを使用する場合，ログアウト機能がサポートされません。

    したがって, SAML2 トークンを使用して別のアプリケーションにアクセスすると，最初のアプリケーションからログアウトするユーザが，2 番目のアプリケーションからログアウトできなくなります。

  - SAML2 トークンの期限切れはアプリケーションのセッション管理に反映されません。

    したがって，SAML2 トークンを使用して別のアプリケーションにアクセスする場合，アプリケーションのセッション管理は個別に処理されます。

- **JAAS Realm**：Tomcat の JAAS Realm はサポートされていません。

- **Tomcat ディレクトリでの空白文字の使用**：Tomcat ディレクトリでは，空白文字はサポートされていません。

  Tomcat インストール・パス（フォルダ）に空白文字が含まれ（「Program Files」など），LW-SSO 構成ファイルが **common¥classes** Tomcat フォルダに格納されていると，LW-SSO は使用できなくなります。

- **負荷分散装置の構成**：LW-SSO を使ってデプロイした負荷分散装置では，スティッキー・セッションを使用する設定が必要です。

第 5 章

ID マネージャの認証

本章の内容

ID マネージャの認証の受信

ID マネージャを使用している環境に HP Universal CMDB Configuration Manager を追加する場合は，次の手順を実行する必要があります。

このタスクでは，ID マネージャによる認証を受信するように，HP Universal CMDB Configuration Manager を構成する方法を説明します。

このタスクでは，次の手順を行います。

前提条件

Configuration Manager Tomcat サーバは，ID マネージャで保護されている Web サーバ（IIS または Apache）に Tomcat Java（AJP13）コネクタで接続します。

Tomcat Java（AJP13）コネクタの使用方法については，Tomcat Java（AJP13）のマニュアルを参照してください。

ID マネージャの使用を HP Universal CMDB Configuration Manager で設定

Tomcat Java（AJP13）と IIS6 を連携する構成を行うために，次の手順を実行します。

1 ユーザ名を含むカスタマイズ・ヘッダ/コールバックを送信する設定を ID マネージャで行い，ヘッダ名を要求します。

2 **＜Configuration Manager インストール・ディレクトリ＞¥conf¥lwssofmconf.xml** ファイルを開き，**in-ui-identity-management** で始まるセクションを探します。

次に例を示します。

```
<in-ui-identity-management enabled="false">
    <identity-management>
      <userNameHeaderName>sm-user</userNameHeaderName>
    </identity-management>
</in-ui-identity-management>
```

a コメント文字を削除して，機能をアクティブにします。

b **enabled="false"** を **enabled="true"** に変更します。

c **sm-user** を，手順 1 で要求したヘッダ名に変更します。

3 **＜Configuration Manager インストール・ディレクトリ＞¥conf¥client-config.properties** ファイルを開き，次のプロパティを編集します。

a **bsf.server.url** を ID マネージャの URL に変更し，ポートを ID マネージャのポートに変更します。

bsf.server.url=http://＜ID マネージャの URL＞:＜ID マネージャのポート＞/bsf

b **bsf.server.services.url** を HTTP プロトコルに変更し，ポートを元の Configuration Manager ポートに変更します。

bsf.server.services.url=http://＜Configuration Manager URL＞:＜Configuration Manager ポート＞/bsf

Configuration Manager 向けの ID マネージャ構成で Java コネクタを使用する例（Windows 2003 オペレーティング・システムで IIS6 を使用）

この例では，Windows 2003 オペレーティング・システムで ISS6 を稼働する環境において，Configuration Manager 用に ID マネージャを設定するためにJava コネクタをインストールおよび構成する方法を説明します。

Java コネクタをインストールし，Windows 2003 環境の ISS6 向けに構成するために，次の手順を実行します。

1 Java コネクタの最新バージョン（**djk-1.2.21** など）を Apache Web サイトからダウンロードします。

   a **http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/** をクリックします。

   b 最新バージョンを選択します。

   c **isapi_redirect.dll** ファイルを **amd64** ディレクトリからダウンロードします。

2 このファイルを**＜Configuration Manager インストール・ディレクトリ＞¥tomcat¥bin¥win32** に保存します。

3 isapi_redirect.dll と同じディレクトリに，**isapi_redirect.properties** という名前で新しいテキスト・ファイルを作成します。

   このファイルの内容は次のとおりです。

   # Jakarta ISAPI Redirector 用の構成ファイル

   # ISAPI Redirector Extension へのパス（Web サイトに対する相対パス）

   # このファイルは，仮想ディレクトリ（実行権限付き）に格納

   extension_uri=/jakarta/isapi_redirect.dll

   # ISAPI Redirector のログ・ファイルへの完全パス

   log_file=＜Configuration Manager インストール・ディレクトリ＞¥servers¥server-0¥logs¥isapi.log

   # ログ・レベル（debug，info，warn，error，trace）

   log_level=info

   # workers.properties ファイルへの完全パス

worker_file==＜Configuration Manager インストール・ディレクトリ＞¥tomcat¥conf¥workers.properties.minimal

uriworkermap.properties ファイルへの完全パス

worker_mount_file==＜Configuration Manager インストール・ディレクトリ＞¥tomcat¥conf¥uriworkermap.properties

4 **＜Configuration Manager インストール・ディレクトリ＞¥tomcat¥conf** に **workers.properties.minimal** という名前のテキスト・ファイルを新しく作成します。

このファイルの内容は次のとおりです。

workers.properties.minimal -

#

このファイルには最小限の jk 構成プロパティを記載

（Tomcat への接続に

必要なプロパティ）

#

名前が ajp13w，タイプが ajp13 のワーカを定義

名前とタイプは必ずしも

一致しない点に注意

worker.list=ajp13w

worker.ajp13w.type=ajp13

worker.ajp13w.host=localhost

worker.ajp13w.port=8009

#END

5 **＜Configuration Manager インストール・ディレクトリ＞¥tomcat¥conf** に **uriworkermap.properties** という名前のテキスト・ファイルを新しく作成します。

このファイルの内容は次のとおりです。

uriworkermap.properties - IIS

#

このファイルにはサンプル・マッピングを記載。例：

```
# ajp13w ワーカ，workermap.properties.minimal で定義
# このファイルの一般的な構文：
# [URL]=[ワーカ名]

/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

重要：Configuration Manager にはルールが 2 つ必要です。新しい構文では，この 2 つを 1 つに統合できます。

/cnc|/*=ajp13w

---

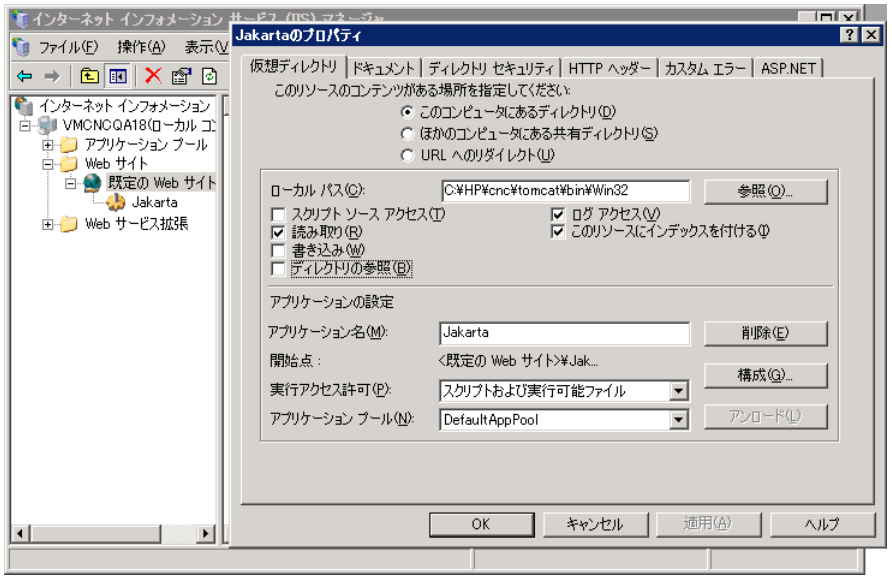
6 IIS 構成で，Web サイト・オブジェクトに仮想ディレクトリを作成します。

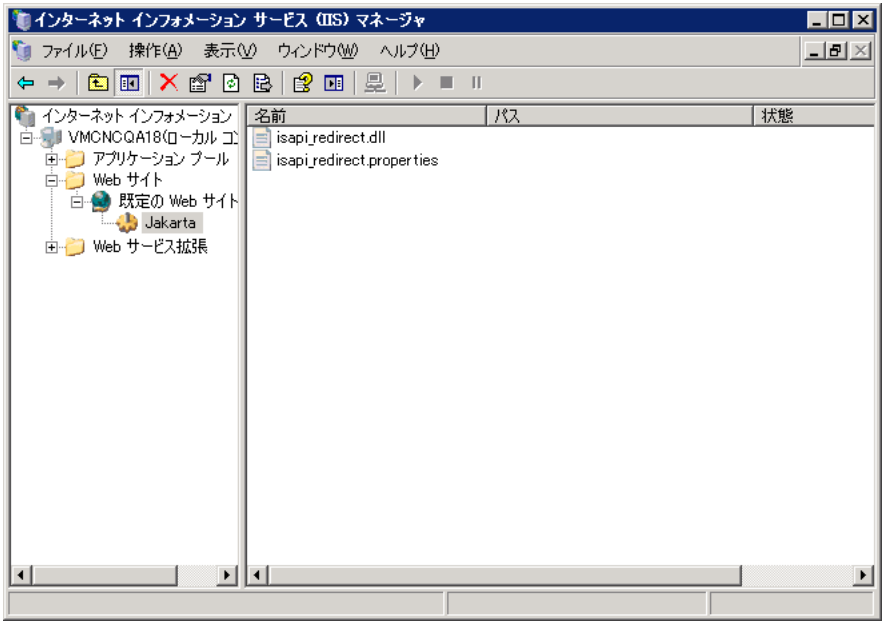
a Windows の［スタート］メニューから［**設定**］＞［**コントロール パネル**］＞［**管理ツール**］＞［**インターネット インフォメーション サービス（IIS）マネージャ**］を選択します。

b 右の表示枠で，**＜ローカル・コンピュータ名＞¥Web サイト¥＜Web サイト名＞**を右クリックして，［**新規作成**］＞［**仮想ディレクトリ**］をクリックします。

c ディレクトリのエイリアス名を「**Jakarta**」と指定し，ローカル・パスには isapi_redirect.dll を含むディレクトリを指定します。

次に，IIS マネージャのウィンドウの例を示します。





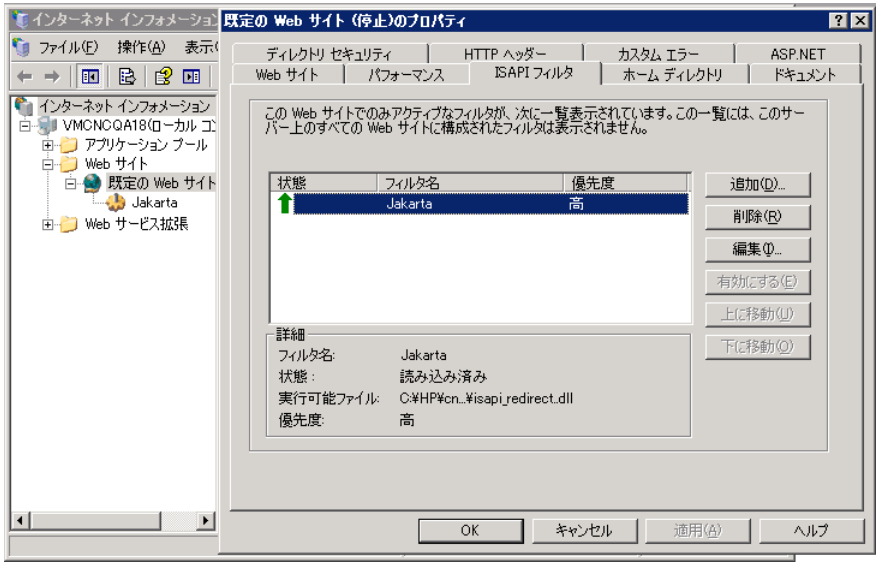
7 ISAPI フィルタに **isapi_redirect.dll** を追加します。

a **＜Web サイト名＞**を右クリックして［**プロパティ**］を選択します。

b ［**ISAPI フィルタ**］タブを選択し，［**追加**］ボタンをクリックします。

c ［フィルタ名］に「**Jakarta**」と入力し，［参照］をクリックして **isapi_redirect.dll** ファイルを指定します。これでフィルタが追加されますが，まだアクティブな状態ではありません。

次のような画面が表示されます。



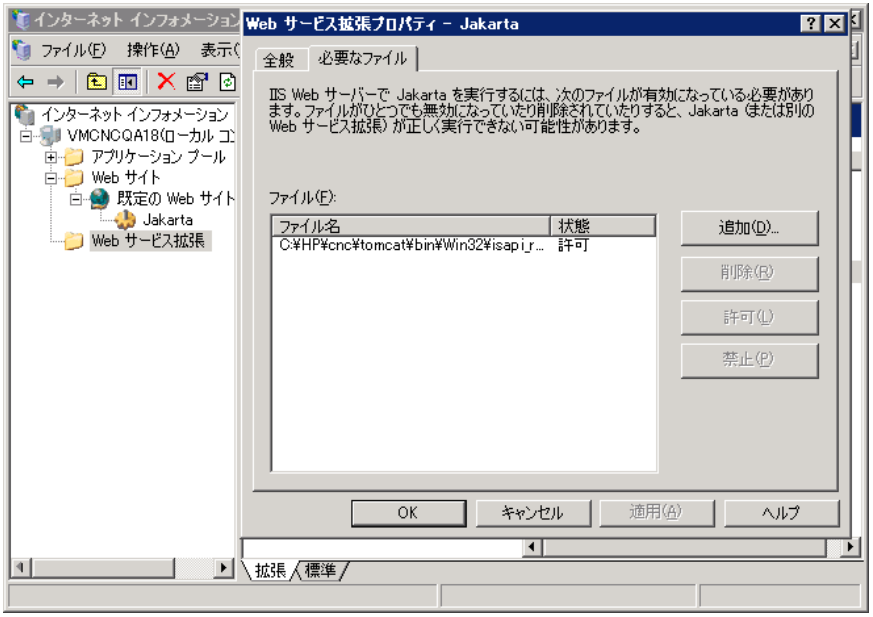
d ［**適用**］ボタンをクリックします。

8 新しい Web サービス拡張を定義し，許可します。

a **＜ローカル コンピュータ名＞¥Web サービス拡張**を右クリックし，［**新しい Web サービス拡張の追加**］メニュー項目を選択します。

b 新しい Web サービス拡張の名前に「**Jakarta**」と入力し，［参照］をクリックして **isapi_redirect.dll** ファイルを指定します。

注：［**拡張の状態を許可済みに設定する**］チェック・ボックスを選択してから，［**OK**］ボタンをクリックします。



9 IIS Web サーバを再起動し，Web サービス経由でアプリケーションにアクセスします。

第 6 章

Configuration Manager へのログイン

本章の内容

Configuration Manager へのアクセス

Configuration Manager には，Configuration Manager サーバへのネットワーク接続（イントラネットまたはインターネット）が設定されたコンピュータから，サポート対象の Web ブラウザを使ってアクセスできます。ユーザに許可されるアクセス・レベルは，ユーザ権限によって決まります。ユーザ権限の割り当てについては，『HP Universal CMDB Configuration Manager ユーザーズ・ガイド』の「ユーザー管理」を参照してください。

Web ブラウザの要件や Configuration Manager を正しく表示するための最低要件の詳細については，8ページ「Configuration Manager のシステム要件」を参照してください。

Configuration Manager へのアクセスでセキュリティを確保する方法については，69ページ「セキュリティの強化」を参照してください。

Configuration Manager へのアクセス方法

Web ブラウザで Configuration Manager サーバの URLを入力します。たとえば，**http://＜サーバ名または IP アドレス＞.＜ドメイン名＞:＜ポート＞**の形式の場合，**＜サーバ名または IP アドレス＞.＜ドメイン名＞**にはConfiguration Manager サーバの完全修飾ドメイン名（FQDN），**＜ポート＞**にはインストール中に選択したポートを指定します。

Configuration Manager へのログイン

1 Configuration Manager Post Installation ウィザードで指定したユーザ名とパスワードを入力します。

2 ［**ログイン**］をクリックします。ログイン後，ユーザ名が画面の右上に表示されます。

3 （推奨）組織 LDAP サーバに接続し，管理者の役割を LDAP ユーザに割り当てます。これにより，Configuration Manager 管理者はシステムにアクセスできるようになります。Configuration Manager のユーザに役割を割り当てる方法については，『HP Universal CMDB Configuration Manager ユーザーズ・ガイド』の「ユーザー管理」を参照してください。

ログアウト

セッションが完了したら，不正な侵入を防ぐため，Web サイトからログアウトします。

ログアウトするには，次の手順を実行します。

ページ上部の［**ログアウト**］をクリックします。

注：セッションの有効期限は，デフォルトで 30 分に設定されています。

JMX コンソールを使った Configuration Manager へのアクセス

トラブルシューティングや一部構成の変更では，JMX コンソールへのアクセスが必要になる場合があります。

JMX コンソールにアクセスするには，次の手順を実行します。

1 http://＜サーバ名または IP アドレス＞:＜ポート＞/cnc/jmx-console にアクセスし，JMX コンソールを開きます。ポートは，Configuration Manager のインストール時に設定したポートを指定してください。

2 デフォルトのユーザ資格情報を入力します。これは，Configuration Manager へのログイン時に使用するユーザ資格情報と同じです。

トラブルシューティングおよび制限事項

問題：［サーバ管理］で構成セットを変更した後，サーバが起動しなくなりました。

解決策：構成セットを変更前の状態に戻します。次の手順を実行してください。

1 次のコマンドを実行し，最後にアクティブ化した構成セットの ID を取得します。

＜HP Universal CMDB Configuration Manager＞¥bin¥export-cs.bat
＜データベース・プロパティ＞ --history

＜データベース・プロパティ＞には，**＜Configuration Manager インストール・ディレクトリ＞¥conf¥database.properties** ファイルの場所を指定するか，各データベース・プロパティを指定します。次に例を示します。

cd ＜HP Universal CMDB Configuration Manager＞¥bin export-cs.bat -p ..¥conf¥database.properties --history

2 次のコマンドを実行し，最後にアクティブ化した構成セットをエクスポートします。

＜HP Universal CMDB Configuration Manager＞¥bin¥export-cs.bat
＜データベース・プロパティ＞ ＜構成セット ID＞ ＜ダンプ・ファイル名＞

＜構成セット ID＞には上記の手順で取得した構成セット ID，**＜ダンプ・ファイル名＞**には構成セットを格納している一時ファイルの名前を指定します。たとえば，ID が **491520** の構成セットを **mydump.zip** ファイルにエクスポートするには，次のコマンドを実行します。

```
cd ＜HP Universal CMDB Configuration インストール・ホーム＞¥bin export-cs.bat
-p ..¥conf¥database.properties -i 491520 -f mydump.zip
```

3 HP Universal CMDB Configuration Manager サービスを停止します。

4 次のコマンドを実行し，上記の構成セットをインポートしてからアクティブ化します。

```
＜HP Universal CMDB Configuration Manager＞¥bin¥import-cs.bat
＜データベース・プロパティ＞ ＜ダンプ・ファイル名＞ --activate
```

問題：UCMDB 接続でエラーが発生します。

解決策：次のいずれかが原因として考えられます。

- ➤ UCMDB サーバが起動していません。UCMDB が完全に稼働状態になってから（UCMDB サーバのステータスが［**Up**］であることを確認），Configuration Manager を再起動します。
- ➤ UCMDB サーバは稼働していますが，Configuration Manager の接続資格情報または URL に誤りがあります。Configuration Manager を起動します。［サーバ管理］を開きます。UCMDB の接続設定を変更し，新しい構成セットとして保存します。構成セットをアクティブ化して，サーバを再起動します。

問題：LDAP 接続設定に誤りがあります。

解決策：構成セットを変更前の状態に戻します。正しい LDAP 接続を設定し，新しい構成セットをアクティブ化します。

問題：UCMDB クラス・モデルの変更が Configuration Manager で検出されません。

解決策：Configuration Manager サーバを再起動します。

問題：Configuration Manager ログに **UCMDB 実行タイムアウト**・エラーが記録されます。

解決策：このエラーは，UCMDB データベースが過負荷状態になると発生します。エラーが発生しないようにするには，接続時間の値を大きくします。

1 jdbc.properties ファイルを **UCMDBServer¥conf** フォルダに作成します。

2 次のように入力します。QueryTimeout=＜秒数＞

3 UCMDB サーバを再起動します。

問題：管理ビューを Configuration Manager に追加できません。

解決策：管理ビューを追加すると，UCMDB で新しい TQL が作成されます。アクティブな TQL の数が上限に達すると，ビューを追加できなくなります。UCMDB でサポートされるアクティブな TQL の最大数を増やすには，インフラストラクチャ設定マネージャで次の値を変更します。

- サーバ内の最大アクティブ TQL 数
- 最大カスタマ アクティブ TQL 数

問題：HTTPS サーバの証明書が無効です。

解決策：次のいずれかが原因として考えられます。

- 証明書の検証日付の期限が切れています。新しい証明書を取得する必要があります。
- 証明書の証明機関が信頼された機関ではありません。信頼されたルート証明機関リストに証明機関を追加してください。

問題：Configuration Manager のログイン・ページからログインすると，ログイン・エラーまたはアクセス拒否ページが表示されます。

解決策：次のいずれかが原因として考えられます。

- ユーザ名が認証プロバイダ（外部/共有 LDAP）で定義されていない可能性があります。ユーザを認証プロバイダ・システムに追加してください。
- ユーザは定義されていますが，Configuration Manager に対するログイン権限が割り当てられていません。ログイン権限を割り当ててください。ベスト・プラクティスとして，すべての Configuration Manager ユーザのルート・グループに，ログイン権限を割り当てる方法が推奨されています。
- 上記の解決方法は，IDM システム・ログインからのログインに失敗した場合にも適用できます。

問題：誤ったデータベース資格情報を入力したことが原因で Configuration Manager サーバが起動しません。

解決策：データベース資格情報を変更した後にサーバが起動しなくなった場合は，資格情報に誤りがある可能性があります。（**注：**Post Installation ウィザードでは，入力した資格情報は自動的にテストされません。［**テスト**］ボタンをクリックする必要があります）。データベース・パスワードを再度暗号化し，新しい資格情報を構成ファイルに入力する必要があります。次の手順を実行してください。

1 コマンド・ラインで次のコマンドを実行し，変更後のデータベース・パスワードを暗号化します。

＜Configuration Manager（CnC）**インストール・フォルダ**＞¥bin¥encrypt-password.bat –p ＜**パスワード**＞

暗号化されたパスワードが返されます。

2 暗号化されたパスワード（{ENCRYPTED} プレフィックスも含む）を**＜CnC インストール・フォルダ＞¥conf¥database.properties** の **db.password** パラメータにコピーします。

問題：DNS の設定に誤りがあると，ログイン時にサーバ IP アドレスを指定する必要がありますが，IP アドレスを入力するとさらに別の DNS エラーが発生します。

解決策：マシン名ではなく IP アドレスを指定します。次に例を示します。

次の IP アドレスを使用してログインします。http://16.55.245.240:8180/cnc/

この場合，DNS エラーが発生し，アドレスとマシン名が表示されます。次に例を示します。http://my.example.com:8180/bsf/secure/authenicationPointURL.jsp...

次のように入力します。http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...

再度，ブラウザでアプリケーションを起動します。

問題：Configuration Manager Tomcat サーバが起動しません。

解決策：次のいずれかの手順を実行してください。

- Post Installation ウィザードを実行して，Configuration Manager サーバ・ポートを変更します。
- Configuration Manager ポートを使用している他のプロセスを中断します。
- Configuration Manager 構成ファイルで指定されているポートを手作業で変更します。**＜CnC インストール・フォルダ＞¥servers¥server-0¥conf¥server.xml**）を編集し，次のポートを変更してください。
  - HTTP (8080)：69 行
  - HTTPS (8443)：71 行，90 行

問題：Configuration Manager ログにメモリ不足エラーが記録されています。

解決策：Java の最大メモリ・サイズを必要に応じて増やします。

Configuration Manager サービスのメモリ・サイズを変更するには, 次の手順を実行します。

1 **＜CnC インストール・フォルダ＞¥cnc¥bin** ディレクトリに移動し，次のコマンドを実行します。edit-server-0.bat

2 ［**Java**］タブを選択します。

3 **Initial memory pool** パラメータと **Maximum memory pool** パラメータを変更します。

バッチ・ファイルのメモリ・サイズを変更するには，次の手順を実行します。

1 **＜CnC インストール・フォルダ＞¥cnc** ディレクトリに移動し，**start-server-0.bat** ファイルを開きます。

2 **SET JAVA_OPTS=-Dcnc.home** で始まる行を検索します。

3 **-Xms** コマンドと **-Xmx** コマンドを探して，適宜変更します。

-Xms＜メモリ・プールの初期サイズ＞ -Xmx＜メモリ・プールの最大サイズ＞

例 : メモリ・プールの初期サイズを 100MB，最大サイズを 800MB に設定するには，次のように入力します。

-Xms100m -Xmx800m

問題 : Post Installation ウィザードで［**完了**］をクリックした後の処理に長時間かかります。

解決策 : 事前に UCMDB システムを統合モードに設定していない場合，スキーマの統合に時間がかかることがあります（データ量によってかかる時間の長さは異なります）。15 分待っても処理が進まない場合，Post Installation ウィザードを中断してプロセスを再開してください。

問題 : UCMDB で CI を変更しましたが，Configuration Manager に反映されません。

解決策 : Configuration Manager で実行される分析プロセスは，オフラインのプロセスであり，非同期的に実行されます。したがって，UCMDB の最新の変更がまだ処理されていない可能性があります。この問題を解決するには，次のいずれかの手順を実行してください。

- 数分間待ちます。分析プロセスの実行間隔は，デフォルトで 10 分に設定されています。この値は，サーバ管理モジュールで設定できます。
- JMX 呼び出しを実行します。これにより，ビューに含まれるオフラインの分析計算が実行されます。
- ポリシー管理にアクセスします。［**ポリシー分析の再計算**］ボタンをクリックします。これにより，オフラインの分析プロセスがすべてのビューで実行されます（多少時間がかかる場合があります）。また，ポリシーを人為的に変更して保存する操作が必要になることもあります。

問題 :［**管理**］＞［**UCMDB を開く**］をクリックすると，UCMDB のログイン・ページが開きます。

解決策 : 再度ログインせずに UCMDB にアクセスするには，シングル・サインオンを有効にする必要があります。詳細については，18ページ「Lightweight シングル・サインオン（LW-SSO）の有効化」を参照してください。さらに，ログインに使用する Configuration Manager ユーザが UCMDB ユーザ管理システムで定義されていることを確認してください。

問題：Post Installation ウィザードで IPv6 アドレスに対する UCMDB 接続を設定しようとすると，［**管理**］＞［**UCMDB を開く**］は使用できなくなります。

解決策：次の手順を実行してください。

1 ［**管理**］＞［**サーバ管理**］＞［**Configuration Manager**］＞［**UCMDB 接続**］を選択します。

2 UCMDB アクセス URL の IP アドレスを角括弧で囲みます。たとえば，http://[x:x:x:x:x:x:x:x]:8080/ のようになります。

3 構成セットを保存し，アクティブ化します。

4 Configuration Manager を再起動します。

Configuration Manager での作業には，次のような制限事項があります。

➤ Configuration Manager Tomcat サーバで時刻を変更した場合は，サーバ上の時刻を更新するために，必ず再起動してください。

第 7 章

セキュリティの強化

本章の内容

Configuration Manager のセキュリティの強化

ここでは，Configuration Manager アプリケーションのセキュリティ保護の概念を紹介し，セキュリティを実装するために必要な計画とアーキテクチャについて説明します。以下の内容を読んでから，セキュリティ強化について説明する後の項に進むことを強くお勧めします。

Configuration Manager は，セキュリティ保護アーキテクチャの一部として使用できるように設計されているので，セキュリティ上の脅威に対処できる機能が用意されています。

セキュリティ強化のガイドラインでは，Configuration Manager のセキュリティ強化に必要な設定作業について取り上げます。

ここで紹介する内容は主に Configuration Manager 管理者を対象としています。セキュリティ強化の作業を開始する前に，セキュリティを強化するための設定や推奨事項について理解するための参考として活用してください。

システムのセキュリティ強化の準備として，次の作業をお勧めします。

- ネットワーク全体でセキュリティ上のリスクやセキュリティの状態を評価し，評価結果に基づいて Configuration Manager をネットワークに統合する最適な方法を検討します。
- Configuration Manager の技術フレームワークと Configuration Manager のセキュリティ機能についてよく理解します。
- セキュリティ強化ガイドラインのすべての内容を検討します。
- Configuration Manager が完全に機能していることを確認してから，セキュリティ強化手順を開始します。
- セキュリティ強化手順は，各項に記載されている順序で実施してください。

重要：

- ここで紹介するセキュリティ強化の手順は，記載内容のみを実施することを前提とするものであり，他で記述されているセキュリティ強化の実施は想定されていません。
- セキュリティ強化手順は特定の分散アーキテクチャを対象としていますが，そのアーキテクチャがユーザ固有の組織のニーズに最適なアーキテクチャであるとは限りません。
- ここで記載する手順は，Configuration Manager 専用のマシンで実行することを想定しています。Configuration Manager 以外の用途にも使用するマシンで実行すると，問題が発生することがあります。
- ここで紹介するセキュリティ強化に関する情報は，ご利用のコンピュータ・システムのセキュリティ・リスクを評価するためのガイドラインではありません。

データベース・パスワードの暗号化

データベース・パスワードは，**＜Configuration Manager インストール・ディレクトリ＞¥conf¥database.properties** ファイルに格納されます。パスワードを暗号化する場合は，FIPS 140-2 標準に準拠した暗号化アルゴリズムがデフォルトで用意されています。データベース・パスワードを暗号化するには，Configuration Manager Post Installation ウィザードの［データベースの設定］ページにある［**パスワードを暗号化する**］チェック・ボックスを選択します。

暗号化の処理としては，まずパスワードがキーを使って暗号化されます。次に，キー自体がマスタ・キーを使って暗号化されます。キーも両方とも同じアルゴリズムを使って暗号化されます。暗号化で使用するパラメータの詳細については，79ページ「暗号化パラメータ」を参照してください。

注意：暗号化アルゴリズムを変更すると，それまでに暗号化したパスワードはすべて使用できなくなります。

データベース・パスワードの暗号化の設定を変更するには，次の手順を実行します。

1 **＜Configuration Manager インストール・ディレクトリ＞¥conf¥encryption.properties** ファイルを開いて次のフィールドを編集します。

- **engineName**：暗号化アルゴリズムの名前を入力します。
- **KeySize**：選択したアルゴリズムのマスタ・キーのサイズを入力します。

2 **generate-keys.bat** スクリプトを実行します。これにより，**cnc¥security¥encrypt_repository** ディレクトリが作成され，暗号化キーが生成されます。

3 Post Installation ウィザードを再度実行します。

自己署名証明書を使用してサーバ・マシンで SSL を有効化

ここでは，Secure Sockets Layer（SSL）チャネルを使用した認証および暗号化をサポートする設定を Configuration Manager で行う方法について説明します。

Configuration Manager は，Tomcat 6.0 をアプリケーション・サーバとして使用します。

注：すべてのディレクトリとファイルの場所は，プラットフォーム，OS，インストール設定によって異なります。

---

1 前提条件

次に示す手順を始める前に，**＜Configuration Manager インストール・ディレクトリ＞¥java¥lib¥security¥tomcat.keystore** にある古い **tomcat.keystore** ファイルを削除してください。

2 サーバ・キーストアの生成

自己署名証明書と秘密鍵を使用してキーストア （JKS タイプ）を作成します。

➤ Java をインストールした **＜Configuration Manager インストール・ディレクトリ＞** の bin ディレクトリで，次のコマンドを実行します。

```
keytool -genkey -alias tomcat -keyalg RSA -keystore
..¥lib¥security¥tomcat.keystore
```

コンソール・ダイアログ・ボックスが開きます。

➤ キーストアのパスワードを入力します。パスワードを変更した場合は，ファイル内のパスワードを手作業で変更します。

➤「**What is your first and last name?**」という質問に回答します。Configuration Manager の Web サーバ名を入力します。組織での指定に基づいて，他のパラメータを入力します。

➤ キーのパスワードを入力します。キーのパスワードには，キーストアのパスワードと同じものを入力してください。

tomcat.keystore という名前の JKS キーストアが作成され，**hpcert** という名前のサーバ証明書が格納されます。

3 クライアントの信頼されたストアに証明書を配置

tomcat.keystore の生成とサーバ証明書のエクスポートが完了したら，自己署名証明書を使用して Configuration Manager と SSL で通信する必要のあるすべてのクライアントについて，この証明書をクライアントの信頼されたストアに配置します。

制限事項：**tomcat.keystore** にはサーバ証明書が 1 つしかない場合があります。

---

4 クライアント構成の確認

＜Configuration Manager インストール・ディレクトリ＞の **conf** ディレクトリにある **client-config.properties** ファイルを開きます。プロトコルを **https**，ポートを **8443** に設定します。

5 server.xml ファイルの変更

＜Configuration Manager インストール・ディレクトリ＞の **conf** ディレクトリにある **server.xml** ファイルを開きます。次の文字列で始まるセクションに移動します。

Connector port="8443"

この部分はコメントになっているので，コメント文字を削除してスクリプトをアクティブにしてから，次の 2 行を追加します。

keystoreFile="＜tomcat.keystore ファイルの格納場所＞"（手順 2（72ページ）を参照してください）

keystorePass="＜パスワード＞"

6 サーバの再起動

7 サーバ・セキュリティの確認

Configuration Manager サーバのセキュリティを確認するには，Web ブラウザで次の URL を入力します。**https://＜Configuration Manager サーバ名または IP アドレス＞:8443/cnc**

ヒント : 接続を確立できない場合は，他のブラウザを使用するか，ブラウザを新しいバージョンにアップグレードしてください。

認証局から取得した証明書を使用してサーバ・マシンで SSL を有効化

認証局（CA）が発行した証明書を使用するには，Java 形式のキーストアが必要です。ここでは，例を使って Windows マシンでキーストアの形式を指定する方法を説明します。

1 前提条件

次に示す手順を始める前に，**＜Configuration Manager インストール・ディレクトリ＞¥java¥lib¥security¥tomcat.keystore** にある古い **tomcat.keystore** ファイルを削除してください。

2 サーバ・キーストアの生成

a 認証局の署名入り証明書を生成し，Windows にインストールします。

b Microsoft 管理コンソール（**mmc.exe**）を使用して，証明書を ***.pfx** ファイルにエクスポートします（秘密鍵を含む）。

➤ **pfx** ファイルのパスワードとして使用する文字列を入力します（キーストアのタイプを JAVA キーストアに変換するとき，このパスワードを入力する必要があります）。
これで，**.pfx** ファイルには公開証明書と秘密鍵が格納され，パスワードで保護された状態になります。

c 作成した **.pfx** ファイルを**＜Configuration Manager インストール･ディレクトリ＞¥java¥lib¥security** フォルダにコピーします。

d コマンド・プロンプトを開き，**＜Configuration Manager インストール・ディレクトリ＞¥bin¥jre¥bin** に移動します。

➤ 次のコマンドを実行し，キーストアのタイプを **PKCS12** から **JAVA** に変更します。

```
keytool -importkeystore -srckeystore ＜Configuration Manager インストール・ディレクトリ＞¥conf¥security¥＜pfx ファイル名＞ -srcstoretype PKCS12 -destkeystore tomcat.keystore
```

変換元（**.pfx**）のキーストアのパスワードを入力するプロンプトが表示されます。手順 b で pfx ファイルを作成したときに指定したパスワードを入力してください。

3 クライアント構成の確認

＜Configuration Manager インストール・ディレクトリ＞¥cnc¥conf¥client-config.properties ファイルを開き，**bsf.server.url** プロパティが **https**，ポートが **8443** に設定されていることを確認します。

4 server.xml ファイルの変更

＜Configuration Manager インストール・ディレクトリ＞¥conf¥server.xml ファイルを開きます。次の文字列で始まるセクションに移動します。

Connector port="8443"

この部分はコメントになっているので，コメント文字を削除してスクリプトをアクティブにしてから，次の 2 行を追加します。

keystoreFile="../../java/lib/security/tomcat.keystore"

keystorePass="password" />

5 サーバの再起動

6 サーバ・セキュリティの確認

Configuration Manager サーバのセキュリティを確認するには，Web ブラウザで次の URL を入力します。**https://＜Configuration Manager サーバ名または IP アドレス＞:8443/cnc**

制限事項：tomcat.keystore にはサーバ証明書が 1 つしかない場合があります。

クライアント証明書を使って SSL を有効化

Configuration Manager Web サーバが使用している証明書がよく知られた認証局 （CA）によって発行されたものである場合，特別な設定を行わなくても Web ブラウザで証明書を検証できる可能性が高くなります。

CA がサーバの信頼ストアによって信頼されていない場合は，CA 証明書をサーバの信頼ストアにインポートする必要があります。

ここでは，自己署名の **hpcert** 証明書をサーバの信頼ストア（cacerts）にインポートする方法を，例を使って説明します。

サーバの信頼ストアに証明書をインポートするには，次の手順を実行します。

1 クライアント・マシンで，**hpcert** 証明書を検索し，名前を **hpcert.cer** に変更します。

Windows エクスプローラを開くと，ファイルがセキュリティ証明書であることを示すアイコンが表示されます。

2 **hpcert.cer** をダブルクリックすると Internet Explorer が起動して［証明書］ダイアログ・ボックスが開きます。ここで，ファイルをインポートします。

3 サーバ・マシン上で keytool ユーティリティを実行し, CA 証明書を信頼ストア（cacerts）にインポートします。次のコマンドを実行してください。

```
keytool.exe -import -alias hp -file hp.cer -keystore ..¥lib¥security¥cacerts
```

4 server.xml ファイルを次のように変更します。

a 手順 5（73ページ）に従って変更を行います。

b 変更した行のすぐ後に，次の行を追加します。

```
truststoreFile="../../java/lib/security/cacerts"
truststorePass="changeit" />
```

c clientAuth="true" を設定します。

5 手順 7（74ページ）に従って，サーバ・セキュリティを確認します。

認証のみで SSL を有効化

このタスクでは，認証のみをサポートするように Configuration Manager を設定する方法を説明します。Configuration Manager を使用するには，このレベルのセキュリティが最低限必要になります。

認証で SSL を有効にするには，次の手順を実行します。

1 72ページ「自己署名証明書を使用してサーバ・マシンで SSL を有効化」から6（74ページ）までの手順，または74ページ「認証局から取得した証明書を使用してサーバ・マシンで SSL を有効化」から5（76ページ）までの手順に従って，サーバ・マシン上で SSL を有効化します。

2 Web ブラウザで次の URL を入力します。
http://＜Configuration Manager サーバ名または IP アドレス＞:8080/cnc

クライアント証明書の認証を有効化

このタスクでは，クライアント側の証明書を認証するために Configuration Manager を設定する方法を説明します。

クライアント証明書の認証を有効化するには，次の手順を実行します。

1 72ページ「自己署名証明書を使用してサーバ・マシンで SSL を有効化」の手順に従って，サーバ・マシン上で SSL を有効にします。

2 **＜Configuration Manager インストール・ディレクトリ＞¥conf¥lwssofmconf.xml** ファイルを開き，in-client certificate で始まるセクションを探します。次に例を示します。

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="e" />
```

コメント文字を削除して，クライアント証明書機能をアクティブにします。

3 次の手順で，証明書からユーザ名を特定します。

a **userIdentifierRetrieveField** パラメータは，証明書のどのフィールドにユーザ名が格納されているかを示します。次のオプションを選択できます。

- **SubjectDN**
- **SubjectAlternativeName**

b **userIdentifierRetrieveMode** パラメータは，フィールドに格納されている内容全体がユーザ名か，一部としてユーザ名が含まれているのかを示します。次のオプションを選択できます。

- **EntireField**
- **FieldPart**

c **userIdentifierRetrieveMode** の値が **FieldPart** の場合，**userIdentifierRetrieveFieldPart** パラメータは，フィールドのどの部分がユーザ名なのかを示します。この値は，証明書内で定義されている凡例に基づくコード文字です。

4 **＜Configuration Manager インストール・ディレクトリ＞¥conf¥client-config.properties** ファイルを開いて次のプロパティを編集します。

- **bsf.server.url** を変更します。72ページ「自己署名証明書を使用してサーバ・マシンで SSL を有効化」の手順に従って，HTTPS プロトコルの使用と HTTPS ポートを設定してください。
- **bsf.server.services.url** を変更します。HTTP プロトコルの使用とオリジナルの HTTP ポートを設定してください。

暗号化パラメータ

次の表は，データベース・パスワードの暗号化で使用するパラメータの一覧です。このパラメータは，**encryption.properties** ファイルで定義されます。データベース・パスワードの暗号化の詳細については，71ページ「データベース・パスワードの暗号化」を参照してください。

パラメータ	説明
cryptoSource	暗号化アルゴリズムを実装するインフラストラクチャを示します。次のオプションを選択できます。 ➤ **lw :** Bouncy Castle（軽量暗号化パッケージ，デフォルト・オプション） ➤ **jce :** Java 暗号化拡張機能（標準の Java 暗号化インフラストラクチャ）
storageType	キーストアのタイプを示します。 現在サポートされているのは, **binary file** のみです。
binaryFileStorageName	ファイル内でマスタ・キーが格納されている場所を示します。
cipherType	暗号のタイプ。現在サポートされているのは, **symmetricBlockCipher** のみです。

パラメータ	説明
engineName	暗号化アルゴリズムの名前。 次のオプションを選択できます。 ➤ **AES**：American Encryption Standard の略。この暗号化方式は FIPS 140-2 に準拠しています(デフォルト・オプション) ➤ **Blowfish** ➤ **DES** ➤ **3DES**：(FIPS 140-2 準拠) ➤ **Null**：暗号化なし
keySize	マスタ・キーのサイズ。このサイズは，アルゴリズムによって異なります。 ➤ **AES**：128，192，256 のいずれか（デフォルトは 256） ➤ **Blowfish**：0-400 ➤ **DES**：56 ➤ **3DES**：156
encodingMode	バイナリ・データの暗号化に使用する ASCII エンコーディング。 次のオプションを選択できます。 ➤ **Base64**（デフォルト・オプション） ➤ **Base64Url** ➤ **Hex**
algorithmModeName	アルゴリズムのモード。現在サポートされているのは，**CBC** のみです。
algorithmPaddingName	使用するパディング・アルゴリズム。 次のオプションを選択できます。 ➤ **PKCS7Padding**（デフォルト・オプション） ➤ **PKCS5Padding**
jceProviderName	JCE 暗号化アルゴリズムの名前。 **注**：指定できるのは，crytpSource が **jce** の場合のみです。**lw** の場合は engineName が使用されます。